数理解析研究所講究録
第 871 巻 1994 年 p.29

A Complexity Theoretic Approach to Breaking Cryptosystems Based on Discrete Logarithms[†]

九州大学 櫻井 幸一
Kouichi SAKURAI [‡]

東北大学 静谷 啓樹
Hiroki SHIZUYA[§]

Abstract

We investigate the complexity of breaking cryptosystems of which security is based on the discrete logarithm problem. We denote the algorithms of breaking the Diffie-Hellman's key exchange scheme by `DH`, the Bellare-Micali's non-interactive oblivious transfer scheme by `BM`, the ElGamal's public-key cryptosystem by `EG`, the Okamoto's conference-key sharing scheme by `CONF`, and the Shamir's 3-pass key-transmission scheme by `3PASS`, respectively. We show a relation among these cryptosystems that

$$\mathtt{3PASS} \leq_m^p \mathtt{CONF} \leq_m^p \mathtt{EG} \equiv_m^p \mathtt{BM} \equiv_m^p \mathtt{DH},$$

where $\leq_m^p$ denotes the polynomial-time many-to-one reducibility. We further gives some condition in which these algorithms have equivalent difficulity. Namely,

1. If the complete factorization of $p-1$ is given, i.e. if the the discrete logarithm problem is a certified one, then these cryptosystems are equivalent with respect to expected polynomial time Turing reducibility.

2. If the underlying group is the Jacobian of an elliptic curve with a prime order, then these cryptosystems are equivalent with respect to polynomial-time many-to-one reducibility.

We also discuss the complexity of several languages related to those computing problems.

[†]A detailed manuscript is available from the authors.

[‡]Department of Computer Science and Communication Engineering, Kyushu University, Hakozaki, Fukuoka 812, Japan. `sakurai@csce.kyushu-u.ac.jp`

[§]ECIP & GSIS, Tohoku University, Kawauchi, Aoba-ku, Sendai 980, Japan `shizuya@ecip.tohoku.ac.jp`